REMARKS

Claims 1-4 and 6-12 stand rejected under 35 U.S.C. §103 as being unpatentable over United States Patent Application Publication No. 2004/0131183 to Sako in view of United States Patent No. 7,392,404 to Montgomery et al. Applicant respectfully traverses this rejection.

Applicants respectfully submit that the cited references fail to disclose or suggest all of the claimed features defined in independent Claims 1 and 12. More specifically, the cited references fail to disclose or suggest a magnetic disk apparatus that includes, *inter alia*, the claimed cipher key unit that erases a first cipher key, and overwrites the first cipher key with a second cipher key in response to a command for discarding all of the first encoded data recorded on the disk medium, as defined in independent Claim 1. The cited references also fail to disclose or suggest a cipher processing method that includes a similar cipher key change step, as defined in independent Claim 12.

In the Sako reference, switching of the cipher key can be achieved only by switching over the address in the memory referred to by the cipher key. However, this does not involve elimination of the cipher key. Therefore, the possibility of the cipher key remaining upon recording in the apparatus (e.g., on a recording medium or a non-volatile memory such as a ROM) cannot be excluded.

In the present invention of independent Claims 1 and 12, the apparatus has a cipher key in it. Since the cipher key is switched over ("overwritt[en]," as now defined in the

amended claims), for example, from cipher key A to cipher key B, the cipher key A reliably disappears from the apparatus after overwriting.

It is one of the objects of the present invention of Claims 1 and 12 to prevent data from being retrieved from the apparatus after the user activates the cipher key change unit/step, such as when discarding or re-selling the apparatus. In an ordinary magnetic disk device, for example, it is possible to analyze the magnetic data of the recording media (magnetic disk) by dismantling the discarded or re-sold device, or by directly extracting out data from a ROM recording firmware or the like. In this case, there is a concern that data can be restored with drawn-out cipher data and cipher key. However, the invention of Claims 1 and 12 eliminates such a concern. In other words, while the configuration of the Sako reference provides a configuration that is insufficient to exclude the risk that the cipher key can be determined, the present invention of Claims 1 and 12 makes it impossible to determine the cipher key before rewriting, even if the cipher key is drawn off after rewriting of the cipher key.

In the Office Action, the Examiner correctly acknowledged that the Sako reference is silent with regard to the claimed feature that recites that the cipher key stored in the cipher key memory unit is erased. Accordingly, the Examiner relied upon the Montgomery et al. reference for this feature. However, as discussed below, even assuming *arguendo* that the Sako reference could be modified in light of the Montgomery et al. reference in the manner suggested by the Examiner, the resulting combination would still not include all of the claimed features.

The Montgomery et al. reference relates to a system of processors having improved integrity and security of data, in which check sum of data stored in the memory is monitored by the use of the processor idle time, and upon detection of an illegal access to the data, a tamper protocol (a protection means against illegal access) is executed.

In certain embodiments of Montgomery et al., the tamper protocol invalidates a port relating to an illegal access. In another embodiment, substantial erasure of data is disclosed by disabling access to data by deleting the key for decoding the data stored in the memory upon detection of an illegal access to data.

In the device of Montgomery et al., the tamper protocol has a configuration for erasing the cipher key. In the present invention of Claims 1 and 12, in contrast, the configuration is such that the user voluntarily instructs, such as from the upper apparatus, to overwrite the cipher key to a new cipher key. More specifically, an important difference between Claims 1 and 12 and Montgomery et al. is that, while in Claims 1 and 12 the cipher key stored in the magnetic disk is deleted (overwritten) in compliance with a command from, for example, the upper apparatus, in the device of the Montgomery et al. reference, the cipher key stored in the memory is deleted by a tamper protocol which is a program on the memory. Accordingly, due to at least these differences between the Montgomery et al. device and the present invention of Claims 1 and 12, Applicant requests the withdrawal of this §103 rejection of independent Claims 1 and 12 and associated dependent Claims 3, 4, and 6-11.

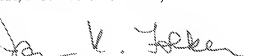
Another difference from the invention of Claims 1 and 12 is that in the devices of the Montgomery et al., there is merely an erasure of the cipher key. In contrast, in the present invention of Claims 1 and 12, there is an overwriting of the cipher key in which a first cipher key is switched to another cipher key. Accordingly, the device of Montgomery et al. cannot be reused as a storage device after the cipher key has been erased, even a single time. In the present invention of Claims 1 and 12, in contrast, even after the cipher key is overwritten from a first cipher key to another cipher key one or more times (i.e., from A to B and from B to C), this only means the annulment of the data at each such rewriting, but even after the rewriting of the cipher key, reuse of the device is possible without impairing the data recording/reproducing function and the cipher function. Accordingly, due to at least these additional differences between the Montgomery et al. device and the present invention of Claims 1 and 12, Applicant requests the withdrawal of this §103 rejection of independent Claims 1 and 12 and associated dependent Claims 3, 4, and 6-11.

For all of the above reasons, Applicant requests reconsideration and allowance of the claimed invention. Should the Examiner be of the opinion that a telephone conference would aid in the prosecution of the application, or that outstanding issues exist, the Examiner is invited to contact the undersigned attorney.

If a Petition under 37 C.F.R. §1.136(a) for an extension of time for response is required to make the attached response timely, it is hereby petitioned under 37 C.F.R. §1.136(a) for an extension of time for response in the above-identified application for the period required to make the attached response timely. The Commissioner is hereby authorized to charge any additional fees which may be required to this Application under 37 C.F.R. §§1.16-1.17, or credit any overpayment, to Deposit Account No. 07-2069.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By 

James K. Folker
Registration No. 37,538

July 6, 2009

Suite 2500
300 South Wacker Drive
Chicago, Illinois 60606
(312) 360-0080

Customer No. 24978